

FILED

SEP 10 4 45 PM '96

Roger Schlafly, Pro Se
PO Box 1680
Soquel, CA 95073
telephone: (408) 476-3550

RICHARD W. WIEKING
CLERK
U.S. DISTRICT COURT
NO. DIST. OF CA, S.J.

In the United States District Court
for the Northern District of California

ROGER SCHLAFLY, Plaintiff) Case C-94-20512 SW PVT
v.)
PUBLIC KEY PARTNERS, and) Proposed Jury Instructions
RSA DATA SECURITY INC., Defendants.) on Stanford Patents
and)
RSA DATA SECURITY INC., Plaintiff) Case C-96-20094 SW PVT
v.)
Cylink, Caro-Kann, and Stanford) Sept. 30, 1996

The parties have agreed to submit proposed jury instructions to
the Court, for argument at the Markman hearing.

Here are my set of proposed instructions. It is somewhat broader
than I expect will actually be given to the jury, because I am
not sure exactly how much the Court is going to narrow these
issues in the Markman hearing.

1 Patent Law
2

3 A patent specification must enable someone of ordinary skill in
4 the art to practice the invention without undue experimentation.
5 It must also describe the best mode known to the inventors.
6

7 For a patent claim to be valid, the specification must enable at
8 least one embodiment which satisfies every element of the claim.
9

10 The scope of a patent claim is limited by each element in the
11 claim. Generic elements are limited by the disclosed embodiments
12 and their equivalents.
13

14 Patent claims must be sufficiently definite to clearly define the
15 set of infringing products.
16

17 Patent claims must be defined and interpreted in a way which is
18 independent of world knowledge or the state of scientific
19 progress.
20

21 Patent claims must be interpreted objectively, and not based on
22 the limited knowledge of the examiner or inventors.
23

24 Two products may be considered equivalent for patent purposes if
25 they perform substantially the same function, in substantially
26 the same way, to obtain substantially the same result.
27
28

1 Definitions

2
3 A "key" is a digitally-encoded number which is used as a control
4 parameter in an encryption or decryption algorithm.

5
6 A "key generator" is a device for generating a new key, not for
7 recovering a key that another party has already generated.

8
9 "Public key" means a key which is meant to be publicly disclosed
10 to potential adversaries with large resources without ruining the
11 promised security. The identification of associated
12 cryptographic algorithms is implied.

13
14 "Secure" means impossible or impractical for an adversary to
15 decrypt intercepted messages. The adversary is assumed to have
16 access to passive interception of ciphertext, large but bounded
17 computational capacity, and the public keys of the parties.

18
19 A function is "feasible" if it is possible for someone to
20 discover an algorithm which can be executed in a practical way on
21 ordinary computer equipment.

22
23 "Computationally infeasible" requires a number of operations (or
24 memory capacity) on an idealized model computer which is too
25 large to be practically executed. The model computer is not too
26 different from real computers. Such numbers mentioned by the
27 inventors are 2^{100} or 10^{30} . Infeasible is the opposite of
28 feasible.

1 Use of "existing computational methods and equipment" refers to
2 computer hardware, but not to hypothetical software programs.

3
4 An essential object of public key cryptography is "demonstrably
5 infeasible cryptanalytic time".

6
7 "Infeasible to invert" means computationally infeasible to find an
8 inverse operation.

9
10
11
12 Dated: Sept 9, 1996

13
14 By: 

15
16 Plaintiff, Roger Schlafly, Pro Se
17
18
19
20
21
22
23
24
25
26
27
28